REMARKS

The Examiner has rejected Claims 1, 21, and 41 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In the Office Action mailed 01/06/2009, the Examiner has reiterated the rejection. Applicant again respectfully points out the clarifications made to the claims in Amendment D mailed 09/24/2008 which avoid such rejection.

Also, in the Office Action mailed 01/06/2009, the Examiner has argued that "it is unclear how exactly 'randomly accessed portion of the requested file' is selected in a random order based on 'portion of the file to be scanned'." Applicant respectfully disagrees and asserts that Claims 1, 21, and 41 specifically recite "data comprising a randomly accessed portion of the requested file selected in a random order...from among portions of the requested file and based on a portion of the requested file to be scanned by the computer malware scanning software" (emphasis added), as claimed. Thus, the "randomly accessed portion of the requested file [is] selected in a random order **from** among portions of the requested file...based on a portion of the requested file to be scanned" (emphasis added), as claimed.

The Examiner has rejected Claims 41-50, 52-60, and 63-64 under 35 U.S.C. 101 as being directed toward non-statutory subject matter. In the Office Action mailed 01/06/2009, the Examiner has simply reiterated the rejection. Applicant again respectfully points out the clarification made to Claim 41 in Amendment D mailed 09/24/2008 which avoids such rejection.

The Examiner has rejected Claims 1-10, 12-30, 32-50, 52-60, and 63 under 35 U.S.C. 103(a) as being unpatentable over Tso et al. (U.S. Patent No. 6,088,803), in view of Fielding et al. ("Hypertext Transfer Protocol - HTTP/1.1," RFC, June 1999). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to the independent claims. Specifically, applicant has

amended the independent claims to at least substantially include the subject matter of former dependent Claims 8 et al. and 9 et al.

With respect to the independent claims, the Examiner has relied on Col. 3, lines 10-54 and Col. 5, lines 1-43 from the Tso reference to make a prior art showing of applicant's claimed "receiving a request from the computer malware scanning software for data comprising a randomly accessed portion of the requested file selected in a random order by the computer malware scanning software from among portions of the requested file and based on a portion of the requested file to be scanned by the computer malware scanning software" (see the same or similar, but not necessarily identical language in the independent claims).

Applicant respectfully notes that the above excerpts from Tso relied on by the Examiner merely teach that "[i]n a typical network transaction, [a] content server... will transmit a requested data object as a series of contiguous portions" (Col. 3, lines 14-16 – emphasis added). Additionally, the above excerpts teach that a "network device... withholds a portion (or a segment of a portion) of the requested file most-recently received from [the] content server... and does not transmit that withheld portion [to the client device] until at least another similarly-sized portion of the requested file is received" (Col. 3, lines 23-28 – emphasis added). Further still, the excerpts teach that a "[v]irus checker... performs virus checking... on the requested file as portions are received from [the] content server" (Col. 3, lines 41-44 - emphasis added). Still yet, applicant respectfully asserts that Col.5, lines 1-43, as relied on by the Examiner, merely relate to "virus checking" where "checked files and/or results of checks may be advantageously stored in a cache storage" (Col. 5, lines 1-3).

However, merely disclosing the transmission of a requested data object as a series of contiguous portions, where a portion of the file most recently received from the content server is withheld until a similarly sized portion is received, and where a virus checker performs virus checking on the requested file as portions are received, as in Tso, fails to disclose "receiving a request from the computer malware scanning software for

data comprising a randomly accessed portion of the requested file selected in a random order by the computer malware scanning software from among portions of the requested file and based on a portion of the requested file to be scanned by the computer malware scanning software" (emphasis added), as claimed by applicant.

In the Office Action mailed 06/25/2008, the Examiner has argued that "Tso teaches [that] a virus checker may be implemented as a software module installed on [a] network device or on a separate device coupled to a network device" and that "[v]irus checking is implemented in a manner intended to maximize efficient transfer of data from server to client device." Additionally, the Examiner has referenced Col. 2, line 38 – Col. 3, line 54 from Tso and has argued that the "[c]ontent server will transmit a requested data object as a series of contiguous portions" and that "[v]irus checker performs virus checking on the requested file as portions are received from content server." Further, the Examiner has argued that "[a]pplicant['s] specification on page 4, line 18-page 5, line 2 teaches that '[t]he requested portion of the requested file may not be transferred because the requested portion of the requested file cannot be randomly accessed [and that a]n indication that the requested portion of the requested file cannot be randomly accessed may comprise an error indication or a transfer of the entire requested file.'" Further still, the Examiner has "interpreted from the above teaching that 'randomly accessed portion of the requested file' can comprise any message other than an error indication or transfer of an entire requested file" and that "[t]herefore, Tso teaches receiving a request [from] the malware scanning software for data comprising [a] randomly accessed portion of the requested file (i.e. a requested data object as a series of contiguous portions)."

Applicant respectfully disagrees. First, applicant notes that the excerpt from the Specification relied on by the Examiner discloses "one aspect of the present invention" where "[t]he requested portion of the requested file may not be transferred because the requested portion of the requested file cannot be randomly accessed" (Page 4, lines 14-20 - emphasis added). However, applicant clearly claims "receiving a request from the computer malware scanning software for data comprising a randomly accessed portion of the requested file selected in a random order by the computer malware scanning software

from among portions of the requested file and based on a portion of the requested file to be scanned by the computer malware scanning software" (emphasis added), as claimed. Of course, the above citations may merely be examples of the above claim language and should not be construed as limiting in any manner.

Additionally, applicant again notes that the Tso reference excerpts relied on by the Examiner merely disclose the transmission of a requested data object as a series of contiguous portions, where a virus checker performs virus checking on the requested file as portions are received, which does not disclose "receiving a request from the computer malware scanning software for data comprising a randomly accessed portion of the requested file selected in a random order by the computer malware scanning software from among portions of the requested file and based on a portion of the requested file to be scanned by the computer malware scanning software" (emphasis added), as claimed by applicant. Merely performing virus checking on contiguous portions as they are received, as in Tso, does not disclose "receiving a request... for data comprising a randomly accessed portion of the requested file selected in a random order by the computer malware scanning software" (emphasis added), as specifically claimed by applicant.

Furthermore, in the Office Action mailed 06/25/2008, the Examiner has argued that "Tso further teaches objects in cache storage may include a virus checking status indicator and a pattern version number... then when a request for a cached object is received, [the] virus checker need only check the parts of the virus pattern file that have changed since the data object was cached." Additionally, the Examiner has relied on Col. 5, lines 27-42 and Col. 9, lines 1-8 of Tso and has argued that "Tso further teaches retrieving a data object to be downloaded to the client, scanning the data object for a computer virus and downloading the data object to the client if no computer virus is detected, wherein the data object is segmented into a series of contiguous portions, retrieving, scanning and downloading steps being performed for each of said contiguous portions."

Applicant respectfully disagrees and notes that the excerpts from Tso relied on by the Examiner merely disclose that "virus checker 5 can maintain a list of deltas in its pattern file" and that "when a request for a cached object is received, virus checker 5 need only check the parts of the virus pattern file that have changed since the data object was cached" (Col. 5, lines 33-37 – emphasis added). Additionally, the excerpts disclose that "the data object is segmented into a series of contiguous portions" and that "said retrieving, scanning and downloading steps [are] performed for each of said contiguous portions" (Col. 9, lines 5-8 – emphasis added).

However, merely disclosing that a virus checker maintains a list of deltas in its virus pattern file, and that only the parts of the virus pattern file that have changed since a data object was cached are checked, as in Tso, fails to even *suggest* "receiving a request from the computer malware scanning software for data comprising a randomly accessed portion of the requested file selected in a random order by the computer malware scanning software from among portions of the requested file and based on a portion of the requested file to be scanned by the computer malware scanning software" (emphasis added), as claimed by applicant. Additionally, applicant again notes that performing scanning on contiguous portions of a segmented data object, as in Tso, does not disclose "receiving a request... for data comprising a randomly accessed portion of the requested file selected in a random order by the computer malware scanning software" (emphasis added), as specifically claimed by applicant.

In the Office Action mailed 01/06/2009, the Examiner has merely reiterated the above rejection, and has thus failed to respond to applicant's specific arguments provided hereinabove. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Additionally, with respect to the independent claims, the Examiner has relied on Page 80, sections 14.24 and 14.25; Pages 82-83, section 14.27; and Pages 85-86, section 14.35 from the Fielding reference to make a prior art showing of applicant's claimed

technique "wherein the randomly accessed portion of the requested file is requested utilizing a byte range technique." More specifically, in the Office Action mailed 06/25/2008, the Examiner has relied on Page 82, section 14.27 and has argued that "Fielding teaches if a client has a partial copy of an entity in its cache (i.e. randomly accessed portion of a file), and wishes [an] up-to-date copy of the entire entity in its cache, it could use range request (i.e. byte range) with a conditional GET."

Applicant respectfully disagrees and notes that the relevant portion of the excerpts relied on by the Examiner merely disclose that "[i]f a client has a partial copy of an entity in its cache, and wishes to have an up-to-date copy of the entire entity in its cache, it could use the Range request-header with a conditional GET" (Page 82, section 14.27 – emphasis added).

However, merely disclosing the use of a Range request-header to obtain a specific portion of an entire entity in a cache, as in Fielding, fails to disclose a technique "wherein the randomly accessed portion of the requested file is requested utilizing a byte range technique" (emphasis added), as claimed by applicant. Nowhere in the above excerpt is "the randomly accessed portion... requested utilizing a byte range technique" (emphasis added), as claimed by applicant.

In the Office Action mailed 01/06/2009, the Examiner has merely reiterated the above rejection, and has thus failed to respond to applicant's specific arguments provided hereinabove. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Further, with respect to the independent claims, the Examiner has relied on Page 80, sections 14.24 and 14.25; Pages 82-83, section 14.27; and Pages 85-86, section 14.35 from the Fielding reference to make a prior art showing of applicant's claimed "tracking information associated with each transfer of a requested portion of the requested file." Additionally, in the Office Action mailed 06/25/2008, the Examiner has relied on Col. 5,

lines 27-42 of Tso and has argued that "Tso teaches cache storage may include a virus checking status indicator and a pattern version number ... then when a request for a cached object is received, virus checker need only check the parts of the virus pattern file that have changed since the data object was cached." Additionally, the Examiner has argued that "Fielding also teaches if the client has no entity tag for an entity, but does not have [a] last modified date, it may use the date in If-range header" and that "[c]hecking entity tag and modified date is adequate to meet the claimed limitation (i.e. tracking information)."

Applicant respectfully disagrees. First, applicant notes that the above reference excerpt from Tso relied on by the Examiner merely discloses that a virus checker maintains a list of deltas in its virus pattern file, and that only the parts of the virus pattern file that have changed since a data object was cached are checked, which fails to even *suggest* "tracking information associated with each transfer of a requested portion of the requested file" (emphasis added), as claimed by applicant.

Additionally, the excerpts from Fielding relied on by the Examiner merely disclose that "[i]f the client has no entity tag for an entity, but does have a Last- Modified date, it MAY use that date in an If-Range header," where "a client has a partial copy of an entity in its cache, and wishes to have an up-to-date copy of the entire entity in its cache" (Page 82, section 14.27 – emphasis added). However, merely determining an entity tag and last-modified date for an entity already existing in the client's cache to use for a new If-Range request header, as in Fielding, fails to disclose "tracking information associated with each transfer of a requested portion of the requested file" (emphasis added), as claimed by applicant.

In the Office Action mailed 01/06/2009, the Examiner has merely reiterated the above rejection, and has thus failed to respond to applicant's specific arguments provided hereinabove. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Further still, with respect to the independent claims, the Examiner has relied on Page 80, sections 14.24 and 14.25; Pages 82-83, section 14.27; and Pages 85-86, section 14.35 from the Fielding reference to make a prior art showing of applicant's claimed technique "wherein the byte range technique turns a serial download mechanism into a random access file mechanism."

Applicant notes that the above reference excerpts relied on by the Examiner merely disclose that "[a] client that has one or more entities previously obtained from the resource can verify that one of those entities is current by including a list of their associated entity tags in the If-Match header field" (Page 80, section 14.24 – emphasis added). In addition, the excerpts disclose that "[t]he If-Modified-Since request-header field is used with a method to make it conditional," where "if the requested variant has not been modified since the time specified in this field, an entity will not be returned from the server" (Page 80, section 14.25 – emphasis added). Additionally, the excerpts merely disclose that "[i]f the client has no entity tag for an entity, but does have a Last-Modified date, it MAY use that date in an If-Range header," where "a client has a partial copy of an entity in its cache, and wishes to have an up-to-date copy of the entire entity in its cache" (Page 82, section 14.27 – emphasis added).

However, disclosing header fields that request the return of an entity if the entity is not current, or if the entity has been modified since a specified time, in addition to disclosing that if a client has a partial copy of an entity in its cache and wishes to have an up-to-date copy of the entire entity, the client may use the Last-Modified date in an If-Range header, as in Fielding, fails to even *suggest* a technique "wherein the byte range technique turns a serial download mechanism into a random access file mechanism" (emphasis added), as claimed by applicant. Nowhere in the above excerpts is "a serial download mechanism [turned] into a random access file mechanism" (emphasis added), as claimed by applicant.

In the Office Action mailed 01/06/2009, the Examiner has merely reiterated the above rejection, and has thus failed to respond to applicant's specific arguments provided hereinabove.

Applicant respectfully emphasizes that the description from Fielding relied on by the Examiner fails to even suggest applicant's claimed technique "wherein the byte range technique turns a serial download mechanism into a random access file mechanism," as claimed. For example, as the Examiner has noted, Fielding only teaches that "one or more entities previously obtained from the resource can verify that one of those entities is current by including a list of their associated entity tags in the If-Match header field" (Page 80 – emphasis added), and that "if a client has a partial copy of an entity in its cache, and wishes to have an up-to-date copy of the entire entity in its cache" the up-to-date copy may be retrieved by the condition "if the entity is unchanged, send me the part(s) that I am missing; otherwise, send me the entire new entity" (Page 82 – emphasis added).

Thus, the above excerpts from Fielding noted by the Examiner merely relate to verifying that an entity is current and requesting an up-to-date copy of an entire entity. Clearly, simply verifying that an entity is current and requesting an up-to-date copy of an entire entity, as in Fielding, does not even suggest a "random access file mechanism" (emphasis added), let alone specifically that "the byte range technique turns a serial download mechanism into a random access file mechanism," as claimed.

Since the Examiner has merely reiterated the aforementioned rejection, as noted above, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Additionally, with respect to the independent claims, the Examiner has argued in the Office Action mailed 06/25/2008 that "Fielding discloses HTTP file transfer protocol consistent with applicant's specification that teaches extensive use of HTTP file transfer protocol." Additionally, the Examiner has cited a paragraph from Page 15 of applicant's

Specification and has further argued that "[t]he examiner has pointed out in the paragraphs discussed above the interpretation of some of the claimed language that is consistent with the specification," that "claims languages are given their broadest reasonable interpretation in view of the specification," and that "[t]herefore, the examiner asserts that cited prior art does teach or suggest the subject matter broadly recited in independent and dependent claims."

Applicant respectfully disagrees. First, applicant again asserts that all of applicant's claim language is to be read according to the plain and ordinary meaning thereof, in view of dictionary definitions, and in further view of the definitions provided in the specification. Further, the above citations may merely be examples of the above claim language and should not be construed as limiting in any manner. Additionally, applicant points out the arguments hereinabove which clearly demonstrate how the references relied on by the Examiner fail to teach or suggest applicant's claim language.

In the Office Action mailed 01/06/2009, the Examiner has merely reiterated the above rejection, and has thus failed to respond to applicant's specific arguments provided hereinabove. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Also, with respect to the independent claims, the Examiner has relied on Page 80, sections 14.24 and 14.25; Pages 82-83, section 14.27; and Pages 85-86, section 14.35 from the Fielding reference to make a prior art showing of applicant's claimed technique "wherein the data associated with the request from the computer malware scanning software comprises a plurality of randomly accessed portions of the requested file."

Applicant respectfully asserts, as argued hereinabove, that the excerpts from Fielding relied upon by the Examiner merely disclose header fields that request the return of an entity if the entity is not current, or if the entity has been modified since a specified time, and additionally disclose that if a client has a partial copy of an entity in its cache

and wishes to have an up-to-date copy of the entire entity, the client may use the Last-Modified date in an If-Range header, which simply does not specifically teach a "plurality of randomly accessed portions of the requested file," much less a technique "wherein the data associated with the request from the computer malware scanning software comprises a plurality of randomly accessed portions of the requested file" (emphasis added) ,as claimed by applicant.

Furthermore, applicant respectfully notes that Col. 3, lines 10-54 and Col. 5, lines 1-43 from the Tso reference, as still relied on by the Examiner on Page 15 of the Office Action mailed 01/06/2009, merely teach that "[i]n a typical network transaction, [a] content server... will transmit a requested data object as a series of contiguous portions" (Col. 3, lines 14-16). Additionally, the above excerpts teach that a "network device... withholds a portion (or a segment of a portion) of the requested file most-recently received from [the] content server... and does not transmit that withheld portion [to the client device] until at least another similarly-sized portion of the requested file is received" (Col. 3, lines 23-28 – emphasis added). Further still, the excerpts teach that a "[v]irus checker... performs virus checking... on the requested file as portions are received from [the] content server" (Col. 3, lines 41-44 – emphasis added). Still yet, applicant respectfully asserts that Col., 5, lines 1-43, as relied on by the Examiner, merely relate to "virus checking" where "checked files and/or results of checks may be advantageously stored in a cache storage" (Col. 5, lines 1-3).

However, merely withholding the most recently received portion of a file from being sent to a client until a similarly-sized portion of the file is received, in addition to performing virus checking on a requested file as portions of the file are received, as in Tso, does not specifically teach a "plurality of randomly accessed portions of the requested file," much less a technique "wherein the data associated with the request from the computer malware scanning software comprises a plurality of randomly accessed portions of the requested file" (emphasis added) ,as claimed by applicant.

In the Office Action mailed 06/25/2008, the Examiner has failed to specifically respond to applicant's above arguments with respect to applicant's claimed technique "wherein the data associated with the request from the computer malware scanning software comprises a plurality of randomly accessed portions of the requested file," as claimed. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

In the Office Action mailed 01/06/2009, the Examiner has merely reiterated the above rejection on Page 15, and has thus failed to specifically respond to applicant's specific arguments provided hereinabove with respect to applicant's claimed technique "wherein the data associated with the request from the computer malware scanning software comprises a plurality of randomly accessed portions of the requested file," as claimed. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the

prosecution of the present application, applicant has at least substantially incorporated the subject matter of former Claims 8 et al. and 9 et al. into the independent claims.

With respect to the subject matter of former Claims 8 et al. and 9 et al. (now at least substantially incorporated into the independent claims), the Examiner has relied on Pages 82-83, section 14.27; and Pages 85-86, section 14.35 from the Fielding reference to make a prior art showing of applicant's claimed "in response to a determination that the requested portion of the requested file cannot be transferred, transferring an entirety of the requested file and supplying the requested data to the computer malware scanning software to fulfill the request for data comprising a portion of the requested file" (see this or similar, but not necessarily identical language in the independent claims from former Claim 8 et al. – as amended) and applicant's claimed technique "wherein it is determined that the requested portion of the requested file cannot be transferred if the requested portion of the requested file cannot be randomly accessed" (see this or similar, but not necessarily identical language in the independent claims from former Claim 9 et al. – as amended). Additionally, in the Office Action mailed 06/25/2008, the Examiner has specifically relied on Page 80, sections 14.24 and 14.25; and Page 82, section 14.27 of Fielding in support of the current rejection.

Applicant again respectfully notes that the above reference excerpts relied on by the Examiner merely disclose that "[a] client that has one or more entities previously obtained from the resource can verify that one of those entities is current by including a list of their associated entity tags in the If-Match header field" (Page 80, section 14.24 – emphasis added). In addition, the excerpts disclose that "[t]he If-Modified-Since request-header field is used with a method to make it conditional," where "if the requested variant has not been modified since the time specified in this field, an entity will not be returned from the server" (Page 80, section 14.25 – emphasis added). Additionally, the excerpts merely disclose that the "meaning [of the If-Range header is] 'if the entity is unchanged, send me the part(s) that I am missing; otherwise, send me the entire new entity'" (Page 82, section 14.27 – emphasis added)

However, merely disclosing header fields that request the return of an entity if the entity is not current, or if the entity has been modified since a specified time, in addition to disclosing a header that requests an entire new entity if the entity has been changed, as in Fielding, does not disclose "in response to a determination that the requested portion of the requested file cannot be transferred, transferring an entirety of the requested file and supplying the requested data to the computer malware scanning software to fulfill the request for data comprising a portion of the requested file" (see this or similar, but not necessarily identical language in the independent claims from former Claim 8 et al. – as amended) and does not disclose a technique "wherein it is determined that the requested portion of the requested file cannot be transferred if the requested portion of the requested file cannot be randomly accessed" (see this or similar, but not necessarily identical language in the independent claims from former Claim 9 et al. – as amended), as claimed by applicant.

In the Office Action mailed 01/06/2009, the Examiner has merely reiterated the above rejection, and has thus failed to respond to applicant's specific arguments provided hereinabove. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Since at least the third element of the *prima facie* case of obviousness has not been met, especially in view of the amendments made hereinabove to the independent claims, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 63, the Examiner has relied on Col. 3, lines 10-54 and Col. 5, lines 1-43 from the Tso reference to make a prior art showing of applicant's claimed technique "wherein the plurality of randomly accessed portions of the requested file are read in a random order."

Applicant again notes that the excerpts from Tso merely disclose withholding the most recently received portion of a file from being sent to a client until a similarly-sized portion of the file is received, in addition to performing virus checking on a requested file as portions of the file are received, as in Tso, which does not specifically teach a "plurality of randomly accessed portions of the requested file," much less a technique "wherein the plurality of randomly accessed portions of the requested file are read in a random order" (emphasis added) ,as claimed by applicant.

In the Office Action mailed 06/25/2008, the Examiner has failed to specifically respond to applicant's above arguments with respect to applicant's claimed technique "wherein the plurality of randomly accessed portions of the requested file are read in a random order," as claimed. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

In the Office Action mailed 01/06/2009, the Examiner has merely reiterated the above rejection, and has thus failed to respond to applicant's specific arguments provided hereinabove. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Further still, the Examiner has rejected Claim 64 under 35 U.S.C. 103(a) as being unpatentable over Tso et al., in view of Fielding et al., and further in view of Ji et al. (U.S. Patent No. 6,728,886). Specifically, the Examiner has relied on Col. 6, line 5 to Col. 8, line 10 of the Ji reference to make a prior art showing of applicant's claimed technique "wherein a system call handler intercepts system level calls made by the computer malware scanning software and simulates system level function calls utilized by the computer malware scanning software to determine whether the requested file includes the computer malware."

Applicant respectfully notes that the above reference excerpt relied on by the Examiner merely teaches the use of auto-config scripts that "detects the HTTP request (e.g., the request for the search page at Yahoo!) and accesses a virus-scan enabling (VSE) server, which in turn dispatches a set of codes capable of creating a local scan engine and or local proxy server..." (Col. 6, lines 25-29) "in order to enable local virus scanning" (Col. 6, lines 55-56). Thus, Ji merely teaches loading and initiating a local virus scanning engine in response to an HTTP request.

However, simply loading and initiating a local virus scanning engine in response to an HTTP request, as disclosed in Ji, fails to teach a technique "wherein a system call handler intercepts system level calls made by the computer malware scanning software and simulates system level function calls utilized by the computer malware scanning software to determine whether the requested file includes the computer malware" (emphasis added), as claimed by applicant.

In the Office Action mailed 06/25/2008, the Examiner has failed to specifically respond to applicant's above arguments with respect to applicant's claimed technique "wherein a system call handler intercepts system level calls made by the computer malware scanning software and simulates system level function calls utilized by the computer malware scanning software to determine whether the requested file includes the computer malware," as claimed. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

In the Office Action mailed 01/06/2009, the Examiner has merely reiterated the above rejection, and has thus failed to respond to applicant's specific arguments provided hereinabove. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Again, since at least the third element of the *prima facie* case of obviousness has not been met, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claim 65 below, which is added for full consideration:

> "wherein scanning by the computer malware scanning software is performed in parallel with transfers of requested portions of the requested file to the malware scanning software" (see Claim 65).

Again, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P664).

Respectfully submitted,
Zilka-Kotab, PC

/KEVINZILKA/

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100